

UNITED STATES DISTRICT COURT

for the

Northern District of Indiana

-FILED-

OCT 06 2023

United States of America

v.

PETRU-RAZVAN BRUMA

Case No.

1:23MJ - 98 - SLC

At _____ M
Chanda J. Berta, Clerk
U.S. DISTRICT COURT
NORTHERN DISTRICT OF INDIANA

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of Between 10/3/23-10/4/23 in the county of Allen in the
Northern District of Indiana, the defendant(s) violated:*Code Section**Offense Description*

18 U.S.C. § 1344

Between on or about October 3, 2023 through and including on or about October 4, 2023, defendant did knowingly execute or attempt to execute a scheme or artifice to defraud Flagstar Bank, a federally insured financial institution, and obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations and promises, and

18 U.S.C. § 1029(a)(4)

Between on or about October 3, 2023 through and including on or about October 4, 2023, defendant did knowingly and with intent to defraud, produce, traffic in, have control or custody of, and possess device making equipment.

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT.

☒ Continued on the attached sheet.Roy M. Stuckey
Complainant's signature

Roy M. Stuckey, FBI Task Force Officer

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/06/2023City and state: Fort Wayne, INs/Susan Collins*Judge's signature*

Susan Collins, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

Comes now Task Force Officer Roy Stuckey of the Federal Bureau of Investigation (FBI), first being duly sworn now deposes and says:

I am a Task Force Officer (TFO) with the FBI. I am an “investigative or law enforcement officer of the United States” within the meaning of 18 U.S.C. §2510(7), and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C. §2516. I am currently responsible for conducting and assisting in investigations into white collar matters including complex financial fraud, public corruption, and health care fraud. During my tenure with the FBI, I have participated in numerous complex narcotic investigations, financial crimes, bank robbery, and other complex frauds. In the past, I have also participated in the execution of search warrants involving physical premises, electronic devices, and other electronic evidence. I have been investigating the current matter since in or about October 3, 2023.

REQUESTED WARRANT

Your affiant requests this Court issue a warrant for the arrest of **PETRU-RAZVAN BRUMA** for alleged violations of 18 U.S.C. §1344 related to bank fraud, and 18 U.S.C. §1029(a)(4) related to fraud and related activity in connection with access devices.

Because this affidavit is being submitted for the limited purpose of securing an arrest warrant for **BRUMA**, your affiant has not included each and every fact known concerning this investigation. This affidavit sets forth only those facts necessary to establish probable cause. The statements in this affidavit are either known to me personally or have been told to me directly by law enforcement officers, witnesses, and other sources. This affidavit is also based in part upon information collected by the Fort Wayne Police Department.

RELEVANT STATUTES

- **18 U.S.C. §1344 – Bank Fraud**

Prohibits knowingly executing or attempting to execute a scheme or artifice to defraud a financial institution or to obtain any of the moneys, funds, credit, assets, securities, or other property owned by, or under the custody or control, a financial institution, by means of false or fraudulent pretenses, representations, or promises.

- **18 U.S.C. §1029(a)(4)**

Prohibits anyone to knowingly and with intent to defraud produce, traffic in, have control or custody of, or possess device-making equipment.

RELEVANT DEFINITIONS

- **Device-making equipment**

Any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device.

18 U.S.C. §1029(e)(6).

- **Access Device**

Any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

18 U.S.C. §1029(e)(1).

- **Skimmer or Skimming Device**

A card reader that can be disguised to look like part of an ATM. The skimmer attachment collects card numbers and PIN codes, which are then replicated into counterfeit cards.

<https://www.nwcu.com/learn/how-spot-atm-skimmer#:~:text=A%20skimmer%20is%20a%20card,is%20compromised%20by%20a%20skimmer.>

PROBABLE CAUSE

The FBI has been investigating several reports of skimming devices being placed on bank ATMs throughout the Northern District of Indiana. Based on your affiant's training and experience and information gathered during this investigation, your affiant knows a skimming device is typically placed on a

card reader and is disguised to appear to be part of the reader. The skimming device is normally by a small camera that is aimed at the credit card keypad to capture the card PIN number input by the customer using the ATM. The skimming device is normally placed on the credit card reader for a short period of time. During this time, the skimming device captures and stores the credit card and debit card numbers of individuals using the ATM to which the skimming device is attached. The camera records the victim typing in their card PIN number. After a period of time, the device and camera are removed from the credit card reader. The information captured and stored by the skimming device is then used to produce fraudulent credit cards and debit cards which are then used to obtain goods, services, or currency.

On October 3, 2023, at approximately 12:45 p.m., your affiant was notified by a representative from Flagstar Bank that a skimming device had been found on an ATM at their branch located at 6324 W Jefferson Blvd, Fort Wayne, Indiana. (Location 1). Flagstar Bank is a “financial institution” as that term is defined in 18 U.S.C. §20. The Flagstar Bank branch located at 6324 W Jefferson Blvd, Fort Wayne, Indiana is in the Northern District of Indiana. The skimming device was discovered by an ATM Service Technician servicing the ATM. The Service Technician discovered the skimming device hanging out of the ATM’s card reader at approximately 12:25p.m. The ATM Service Technician notified bank security who then contacted law enforcement officers.

When law enforcement officers arrived, the skimming device and a camera were removed from the ATM.

A representative of Flagstar Bank provided bank surveillance camera video of the individual placing the skimming device on the ATM at Location 1 as well as the vehicle that individual was driving. Bank surveillance video showed that on October 3, 2023, at approximately 7:40 a.m., a gray 2022 Chevrolet Malibu bearing New York license plate KBU3496(gray Malibu), registered to PV Holding Corp., arrived at the ATM at Location 1. The driver of the gray Malibu then got out of the car. The individual was wearing a dark colored baseball hat with two light blue stripes and four red stars, a white Calvin Klein t-shirt, dark colored pants, a black mask, and sunglasses. When the individual exited the gray Malibu, he was carrying a long chrome colored item that was later determined by law enforcement officers to be a camera that could be affixed to the ATM to capture a customer's PIN number as the customer puts the PIN number into the ATM. The individual placed the camera on the ATM. At approximately 7:40 a.m., the individual departed Location 1 driving the gray Malibu.

At approximately 8:10 a.m., the gray Malibu arrived at a Flagstar Bank stand- alone ATM located 6218 St. Joe Center Road (Location 2). 6218 St. Joe Center Road is also in the Northern District of Indiana. The same individual from Location 1 exited the gray Malibu. The individual was wearing the same

clothes described above as having been worn by the individual placing the skimming device and camera on the ATM at Location 1. The individual placed on the ATM at Location 2 what appeared to be a camera similar to that placed on the ATM at Location 1. The ATM surveillance video then showed the individual place a skimming device into the card slot of the ATM at Location 2. That individual then got back into the gray Malibu and left the area.

On October 3, 2023, at approximately 3:43 a.m., a commercially available license plate database had identified the gray Malibu departing the area of the intersection of North Kenmore Avenue and West Hollywood Avenue in Chicago, Illinois. After placing the skimming device on the ATM at Location 2, the gray Malibu was identified by the same license plate database as arriving back in the Chicago, Illinois area at approximately 10:06 a.m. on October 3, 2023. The license plate database also identified that the gray Malibu had again returned to the intersection of North Kenmore Avenue and West Hollywood Avenue in Chicago, Illinois at approximately 10:55 p.m. on October 3, 2023.

On October 4, 2023, a commercially available license plate database identified the gray Malibu departing the area of the intersection of North Kenmore Avenue and West Hollywood Avenue in Chicago, Illinois at approximately 3:32 p.m. At approximately 7:48 p.m., surveillance officers observed the gray Malibu arrive in the vicinity of Location 1. The gray Malibu

passed Location 1 and parked in a nearby Burger King parking lot which is located at 6402 W Jefferson Blvd, Fort Wayne, Indiana. The individual from the gray Malibu got out of the gray Malibu and entered the Burger King. At approximately 7:51 p.m., the same individual exited Burger King, got back into the gray Malibu, and left the area.

At approximately 8:13 p.m., the gray Malibu arrived at Location 2 and pulled up to the ATM at Location 2. The individual driving the gray Malibu exited the gray Malibu and approached the ATM. The individual appeared to do something at the ATM, but it does not look like the individual made a transaction while at the ATM. The individual then got back into the gray Malibu and left the area. At approximately 8:31 p.m., officers from the Fort Wayne Police Department conducted a traffic stop of the gray Malibu for traveling 70mph in a 50mph zone as it headed westbound on U.S. 30 near O'Day Road. That location is also in the Northern District of Indiana. The driver presented law enforcement with a driver's license from the United Kingdom in the name of Petru-Razvan **Bruma**. Officers observed that **Bruma** wearing a dark colored baseball hat with two light blue stripes and four red stars. This is the same type of hat seen being worn by the individual placing the skimming device and cameras at Location 1 and Location 2. Law enforcement also noticed that **Bruma** had hanging from his white t-shirt a pair of sunglasses similar in style to the sunglasses worn by the individual

placing the skimming devices and cameras at Location 1 and Location 2. **Bruma** told officers he was on his way to Chicago and was coming from Columbus, Ohio after visiting friends for a short period of time. Law enforcement had **Bruma** exit the gray Malibu to speak with your affiant. Your affiant asked **Bruma** about the gray Malibu. **Bruma** told affiant that he had rented the gray Malibu in his name approximately two weeks prior from Budget/Avis at Midway Airport in Chicago, Illinois. **Bruma** also told officers he had not been in Fort Wayne, Indiana on October 3, 2023, and that he did not use any ATMs on that day. **Bruma** said that he was the only person that drove the gray Malibu. However, after being asked about the skimmers, **Bruma** went on to say that he stays at a house with roommates and one of them may have taken the gray Malibu. Officers placed Bruma under arrest and he was transported to the Allen County Jail.

Based on a comparison between the bank surveillance video from Location 1 and Location 2 and **Bruma**, it is your affiant's opinion that the individual placing the skimming devices and cameras on the Flagstar ATMs on October 3, 2023, was **Petru-Razvan Bruma**.

CONCLUSION

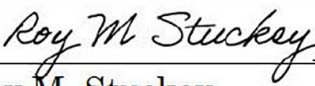
Based on the above information, your affiant has probable cause to believe that:

- Between on or about October 3, 2023 through and including on or about October 4, 2023, defendant did knowingly execute or attempt to execute a scheme or artifice to defraud Flagstar Bank, a federally insured financial institution, and obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations and promises, in violation of 18 U.S.C. §1344; and
- Between on or about October 3, 2023, through and including on or about October 4, 2023, defendant did knowingly and with intent to defraud, produce, traffic in, have control or custody of, and possess device making equipment, in violation of 18 U.S.C. §1029(a)(4).

The foregoing facts are true to the best of your affiant's knowledge and belief.


This complaint affidavit and arrest warrant are being considered and executed by reliable electronic means under Federal Rule of Criminal Procedure 4.1.

Further you affiant sayeth naught.



Roy M. Stuckey
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn before me this 6th day of October 2023.



Hon. Susan Collins
U.S. Magistrate Judge
Northern District of Indiana

